QUADRATIC RESIDUES IN FIBONACCI SEQUENCES

ALEXANDRU GICA

Abstract. In this paper we find all the prime numbers p for which there exists a Fibonacci sequence modulo p, $(a_n)_{n>0}$, such that this sequence modulo p is the set of the quadratic residues modulo p.

1. Introduction

Let us first consider the sequence $1, 4, 5, 9, 3$. These are the quadratic residues modulo 11 and we observe that each number of this sequence is the sum, modulo 11, of the previous two (and $9 + 3 \equiv 1 \pmod{11}$, $3 + 1 \equiv 4 \pmod{11}$). Similarly, if we consider the sequence $1, 5, 6, 11, 17, 9, 7, 16, 4$, these are the quadratic residues modulo 19 and each number of this sequence is the sum, modulo 19, of the previous two (and $16 + 4 \equiv 1 \pmod{19}$, $4 + 1 \equiv 5 \pmod{19}$). We are asking which are the numbers which have the same property as 11 and 19. Therefore we consider the following.

Problem. Which are the prime numbers $p > 2$ such that there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{2}$ and

$$\{\overline{a_n} | n \in \mathbb{N}^*\} = \{b^2 | b \in \mathbb{F}_p^*\}?$$

In the above formula, $\mathbb{F}_p^*$ is the multiplicative group of the field of the residues modulo p and $\overline{a_n}$ means the class of a_n modulo p. If p is a prime number, $p \equiv 1, 4 \pmod{5}$, then the Legendre symbol $\left(\frac{5}{p}\right)$ is 1 and so there exists a positive integer $m \leq \frac{p-1}{2}$ such that $5 \equiv m^2 \pmod{p}$. We will denote this number m by $\sqrt{5}$.

We will prove the following result.

Theorem 1.1. *If $p > 2$ is a prime number, there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{2}$ and $\{\overline{a_n} | 1 \leq n \leq \frac{p-1}{2}\} = \{b^2 | b \in \mathbb{F}_p^*\}$ if and only if*

i) $p \equiv 1, 4 \pmod{5}$ *and*

ii) *ord* $\alpha = \frac{p-1}{2}$ *or ord* $\beta = \frac{p-1}{2}$, *where* $\alpha = \frac{1+\sqrt{5}}{2}$ *and* $\beta = \frac{1-\sqrt{5}}{2}$.

As above, $\sqrt{5}$ means the unique positive integer $m \leq \frac{p-1}{2}$ such that $5 \equiv m^2 \pmod{p}$. The orders ord α and ord β are considered in the multiplicative group $\mathbb{F}_p^*$.

If $p \equiv 1, 4 \pmod{5}$ and *ord* $\alpha = \frac{p-1}{2}$ or *ord* $\beta = \frac{p-1}{2}$, then it is easy to check the statement of the theorem since $\alpha^2 \equiv \alpha + 1 \pmod{p}$, $\beta^2 \equiv \beta + 1 \pmod{p}$. If *ord* $\alpha = \frac{p-1}{2}$, then the sequence $(a_n)_{n>0}$ is $a_n = \alpha^n$. Since $\alpha^2 \equiv \alpha + 1 \pmod{p}$, we have $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$.

Since $ord\ \alpha = \frac{p-1}{2}$, then we have from Euler's Criterion that $1 \equiv \alpha^{\frac{p-1}{2}} \equiv \left(\frac{\alpha}{p}\right) \pmod{p}$ and $\left(\frac{\alpha}{p}\right) = 1$; this means that all the powers of α are quadratic residues modulo p.

This ends the proof. If $ord\ \beta = \frac{p-1}{2}$, then the sequence $(a_n)_{n>0}$ is $a_n = \beta^n$ and we check in the same way as above the statement of the theorem. Therefore we have to prove only one implication. In the sequel we suppose that $p > 2$ is a prime such that there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{2}$ and $\{\overline{a_n} | n \in \mathbb{N}^*\} = \{b^2 | b \in \mathbb{F}_p^*\}$. From the last condition we deduce that p does not divide a_n for any positive integer n. Replacing the sequence $(a_n)_{n>0}$ with the sequence $(b_n = \frac{a_n}{a_1})_{n>0}$ which has the same properties as the initial one, we can suppose that $a_1 = 1$ and $a_2 = x \not\equiv 1 \pmod{p}$. □

2. First step: Proving that $p \equiv 1, 4 \pmod{5}$.

We will now show the first statement of the theorem.

Proof. Obviously, the prime $p = 5$ does not have the properties stated in the theorem. Let us suppose now that $\left(\frac{5}{p}\right) = -1$. We have

$$a_{n+2} = F_n + xF_{n+1}, \tag{2.1}$$

for all positive integers n, where F_n is the Fibonacci sequence. We know that $(a_n)_{n>0}$ modulo p is periodic with period $\frac{p-1}{2}$. Hence,

$$x = a_2 \equiv a_{p+1} = F_{p-1} + xF_p \pmod{p}, \ \ 1 + x = a_3 \equiv a_{p+2} = F_p + xF_{p+1} \pmod{p}. \tag{2.2}$$

We have the well-known Catalan's formula (see [1], p. 157)

$$2^{n-1}F_n = C_n^1 + C_n^3 5 + C_n^5 5^2 + \cdots \tag{2.3}$$

where the C_n^k are the binomial coefficients $\binom{n}{k}$. If we put in the last equality $n = p$, then we have

$$2^{p-1}F_p = C_p^1 + C_p^3 5 + C_p^5 5^2 + \cdots + C_p^p 5^{\frac{p-1}{2}}. \tag{2.4}$$

Since $2^{p-1} \equiv 1 \pmod{p}$ and the binomial coefficients C_p^j are multiples of p for any $j = \overline{1, p-1}$, from the equation (2.4) it follows that $F_p \equiv 5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) = -1 \pmod{p}$. If we put in equation (2.3) $n = p + 1$, we obtain

$$2^p F_{p+1} = C_{p+1}^1 + C_{p+1}^3 5 + C_{p+1}^5 5^2 + \cdots + C_{p+1}^p 5^{\frac{p-1}{2}}. \tag{2.5}$$

Since p divides C_{p+1}^j for any $2 \le j \le p-1$ and $2^p \equiv 2 \pmod{p}$ then $2F_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} \equiv 1 + \left(\frac{5}{p}\right) = 0 \pmod{p}$. We obtain

$$F_p \equiv -1 \pmod{p}, \ F_{p+1} \equiv 0 \pmod{p}, \ F_{p-1} = F_{p+1} - F_p \equiv 1 \pmod{p}.$$

Replacing these values in formula (2.2), it follows that $1 + x = a_3 \equiv a_{p+2} = F_p + xF_{p+1} \equiv -1 \pmod{p}$, so that

$$x \equiv -2 \pmod{p}$$

and $x = a_2 = a_{p+1} = F_{p-1} + xF_p \equiv 1 - x \pmod{p}$, $2x \equiv 1 \pmod{p}$. Combining this last congruence with $x \equiv -2 \pmod{p}$, it follows that $2(-2) \equiv 1 \pmod{p}, p = 5$, which is a contradiction. We proved that $p \equiv 1, 4 \pmod{5}$. □

3. The case $p \equiv 3 \pmod 4$.

We will prove the second statement of the theorem in the case when $p \equiv 3 \pmod 4$.

Proof. We have the classical Binet's formula (see [1], p. 155)

$$F_n \equiv \frac{1}{\sqrt{5}}\left(\alpha^n - \left(-\frac{1}{\alpha}\right)^n\right) \pmod p. \tag{3.1}$$

Putting in the above formula $n = \frac{p+1}{2}$ and taking into account the fact that $\frac{p+1}{2}$ is an even number and that $\alpha^{p-1} \equiv 1 \pmod p$ we obtain

$$F_{\frac{p+1}{2}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p+1}{2}} - \frac{1}{\alpha^{\frac{p+1}{2}}}\right) \equiv \frac{1}{\sqrt{5}}\frac{\alpha^2-1}{\alpha^{\frac{p+1}{2}}} \equiv \frac{1}{\sqrt{5}}\frac{\alpha}{\alpha^{\frac{p+1}{2}}} \equiv \frac{1}{\sqrt{5}}\frac{1}{\alpha^{\frac{p-1}{2}}} \pmod p. \tag{3.2}$$

Putting in formula (3.1) $n = \frac{p-1}{2}$ and taking into account the fact that $\frac{p-1}{2}$ is an odd number and that $\alpha^{p-1} \equiv 1 \pmod p$ we obtain

$$F_{\frac{p-1}{2}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2}} + \frac{1}{\alpha^{\frac{p-1}{2}}}\right) \equiv \frac{1}{\sqrt{5}}\frac{2}{\alpha^{\frac{p-1}{2}}} \pmod p. \tag{3.3}$$

Since the sequence $(a_n)_{n>0}$ modulo p has period $\frac{p-1}{2}$ we have

$$x = a_2 \equiv a_{\frac{p+3}{2}} = F_{\frac{p-1}{2}} + xF_{\frac{p+1}{2}} \pmod p, \quad x(1 - F_{\frac{p+1}{2}}) \equiv F_{\frac{p-1}{2}} \pmod p. \tag{3.4}$$

Case 1. $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod p$. In this case, from formulas (3.2) and (3.3) it follows that $F_{\frac{p+1}{2}} \equiv \frac{1}{\sqrt{5}} \pmod p$ and $F_{\frac{p-1}{2}} \equiv \frac{2}{\sqrt{5}} \pmod p$. Putting these values in formula (3.4) we obtain $x(1 - \frac{1}{\sqrt{5}}) \equiv \frac{2}{\sqrt{5}} \pmod p$ and

$$x \equiv \frac{2}{\sqrt{5}-1} \equiv \frac{\sqrt{5}+1}{2} = \alpha \pmod p.$$

Therefore, $a_2 = x, a_3 = 1 + x \equiv 1 + \alpha \equiv \alpha^2 \pmod p$ and by induction we infer that $a_n \equiv \alpha^n \pmod p$ for any positive integer n. From the condition of the hypothesis it follows now immediately that $ord\, \alpha = \frac{p-1}{2}$.

Case 2. $\alpha^{\frac{p-1}{2}} \equiv -1 \pmod p$. In this case, from formulas (3.2) and (3.3) it follows that $F_{\frac{p+1}{2}} \equiv -\frac{1}{\sqrt{5}} \pmod p$ and $F_{\frac{p-1}{2}} \equiv -\frac{2}{\sqrt{5}} \pmod p$. Putting these values in formula (3.4) we obtain $x(1 + \frac{1}{\sqrt{5}}) \equiv -\frac{2}{\sqrt{5}} \pmod p$ and

$$x \equiv -\frac{2}{\sqrt{5}+1} \equiv \frac{-\sqrt{5}+1}{2} = \beta \pmod p.$$

Therefore, $a_2 = x, a_3 = 1 + x \equiv 1 + \beta \equiv \beta^2 \pmod p$ and by induction we infer that $a_n \equiv \beta^n \pmod p$ for any positive integer n. From the condition of the hypothesis it follows immediately that $ord\, \beta = \frac{p-1}{2}$. □

4. The case $p \equiv 1 \pmod 4$.

We will show first that $\left(\frac{\alpha}{p}\right) = 1$ in this case.

Proof. From formula (3.1) it follows that

$$F_{\frac{p-1}{2}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p-1}{2}} - \frac{1}{\alpha^{\frac{p-1}{2}}}\right) \equiv 0 \pmod p \tag{4.1}$$

and from formula (3.4) we infer that $F_{\frac{p+1}{2}} \equiv 1 \pmod p$. Let us suppose that $\left(\frac{\alpha}{p}\right) = -1$. From formula (3.1) it follows that

$$F_{\frac{p+1}{2}} \equiv \frac{1}{\sqrt{5}}\left(\alpha^{\frac{p+1}{2}} + \frac{1}{\alpha^{\frac{p+1}{2}}}\right) \equiv -\frac{1}{\sqrt{5}}\frac{\alpha^2+1}{\alpha} \equiv -\frac{1}{\sqrt{5}}\frac{\alpha\sqrt{5}}{\alpha} \equiv -1 \pmod p. \tag{4.2}$$

In the above proof we used $\alpha^2 + 1 \equiv \alpha\sqrt{5} \pmod p$. Formula (4.2) does not fit with what we obtained above: $F_{\frac{p+1}{2}} \equiv 1 \pmod p$. Therefore we have proved that $\left(\frac{\alpha}{p}\right) = 1$ in this case.

We will show that $ord\,\alpha = \frac{p-1}{2}$ or $ord\,\beta = \frac{p-1}{2}$. Let us denote $d = ord\,\alpha$ in $\mathbb{F}_p^*$. Since $\left(\frac{\alpha}{p}\right) = 1$, we infer from Euler's Criterion that $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod p$ and therefore d divides $\frac{p-1}{2}$. We have $\frac{p-1}{2} = kd$, where $k \in \mathbb{N}^*$. If $k = 1$, we have proved the theorem. Let us suppose now that $k \geq 2$. From formula (3.1) it follows that $F_{n+2d} \equiv F_n \pmod p$ for any positive integer n and that $a_{n+2d} \equiv a_n \pmod p$ for any positive integer n. Since the period of $(a_n)_{n>0}$ modulo p is $\frac{p-1}{2}$, it follows that $2d \geq \frac{p-1}{2} = kd, 2 \geq k \geq 2, k = 2, d = \frac{p-1}{4}$. Let us show now that in this case $d = \frac{p-1}{4}$ is odd. Indeed, if d would be even, then from formula (3.1) it would follow that $F_{n+d} \equiv F_n \pmod p$ for any positive integer n and that $a_{n+d} \equiv a_n \pmod p$ for any positive integer n. It would result that the period of $(a_n)_{n>0}$ modulo p would be smaller than $d = \frac{p-1}{4}$ which is false since the period of $(a_n)_{n>0}$ modulo p is $\frac{p-1}{2}$. Then d is odd. We will show now that $ord\,\beta = \frac{p-1}{2}$. Let us denote $d_1 = ord\,\beta$ in $\mathbb{F}_p^*$. We have

$$\beta^{\frac{p-1}{2}} = \left(-\frac{1}{\alpha}\right)^{\frac{p-1}{2}} = \frac{1}{\alpha^{\frac{p-1}{2}}} \equiv 1 \pmod p \tag{4.3}$$

and therefore d_1 divides $\frac{p-1}{2}$. We have

$$1 \equiv \beta^{2d_1} = \left(-\frac{1}{\alpha}\right)^{2d_1} = \frac{1}{\alpha^{2d_1}} \pmod p$$

and therefore, $\alpha^{2d_1} \equiv 1 \pmod p$ and $\frac{p-1}{4} = d = ord\,\alpha$ divides $2d_1$. Since d is odd, it follows that d divides d_1 and from (4.3) it follows that d_1 divides $\frac{p-1}{2}$. We infer that $d_1 = \frac{p-1}{4}$ or $d_1 = \frac{p-1}{2}$. If $d_1 = \frac{p-1}{4}$, then (since $d = d_1$ is odd)

$$1 \equiv \beta^{d_1} = \left(-\frac{1}{\alpha}\right)^{d_1} = -\frac{1}{\alpha^d} \equiv -1 \pmod p,$$

which is a contradiction. Therefore, $d_1 = \frac{p-1}{2} = ord\,\beta$ and we finished the proof of the theorem. □

Remark. *The first prime number* $p \equiv 1, 4 \pmod 5$ *which does not have the property stated in Theorem 1.1 is* $p = 41$. *In this case* $\sqrt{5}$ *is 13 since* $13^2 \equiv 5 \pmod{41}$. *Hence,* $\alpha = \frac{1+\sqrt{5}}{2} = 7$ *and* $\beta = \frac{1-\sqrt{5}}{2} = -6$. *We have* $\alpha^{20} \equiv \left(\frac{7}{41}\right) = -1 \pmod{41}$, $\beta^{20} \equiv \left(\frac{-6}{41}\right) = -1 \pmod{41}$ *and* α *and* β *do not have order 20.*

5. Another result and a Conjecture.

Following the same path as above we can prove the following result.

Theorem 5.1. *If $p > 2$ is a prime number, there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $p - 1$ and $\{\overline{a_n} | 1 \le n \le p - 1\} = \mathbb{F}_p^*$ if and only if*
i) $p \equiv 1, 4 \pmod{5}$ and
ii) ord $\alpha = p - 1$ or ord $\beta = p - 1$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. As above, $\sqrt{5}$ means the unique positive integer $m \le \frac{p-1}{2}$ such that $5 \equiv m^2 \pmod{p}$.

The above two results suggest to study the following.

Conjecture. *If $p > 2$ is a prime number and k is a divisor of $p - 1$, there exists a sequence $(a_n)_{n>0}$ such that $a_{n+2} \equiv a_{n+1} + a_n \pmod{p}$ for any positive integer n, a_n is periodic modulo p with period $\frac{p-1}{k}$ and $\{\overline{a_n} | 1 \le n \le \frac{p-1}{k}\} = \{b^k | b \in \mathbb{F}_p^*\}$ if and only if*
i) $p \equiv 1, 4 \pmod{5}$ and
ii) ord $\alpha = \frac{p-1}{k}$ or ord $\beta = \frac{p-1}{k}$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. As above, $\sqrt{5}$ means the unique positive integer $m \le \frac{p-1}{2}$ such that $5 \equiv m^2 \pmod{p}$.

References

[1] A. Gica and L. Panaitopol, *O Introducere în Aritmetică şi Teoria Numerelor*, Bucharest University Press, Bucharest, 2001.

MSC2000: 11A15, 11B39

Faculty of Mathematics and Computer Science, University of Bucharest, Bucharest 1, Str. Academiei 14, RO-010014, Romania
E-mail address: alexgica@yahoo.com